Exhibit B

NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
ONE STATE STREET
NEW YORK, NEW YORK 10004

----------x

In the Matter of :

NORDEA BANK ABP, and :
NORDEA BANK ABP NEW YORK BRANCH

:

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department"), Nordea Bank Abp, and the New York Branch of Nordea Bank Abp (the "New York Branch" or the "Branch") (collectively, "Nordea" or "the Bank") are willing to resolve the matters described herein without further proceedings.

WHEREAS, Nordea is a global banking and financial services institution headquartered in Helsinki, Finland;

WHEREAS, Nordea Bank Abp is licensed by the Department to operate a foreign bank branch in the State of New York;

WHEREAS, prior to October 2017, Nordea had branches in Latvia (Nordea Bank AB Latvia, the "Latvian Branch"), Lithuania (Nordea Bank Abp Lithuania, the "Lithuanian Branch"), and Estonia (Nordea Bank Abp Estonia Branch, the "Estonian Branch") (together the "Baltic Branches"), and the Vesterport International Branch at Vesterport, Denmark ("VIB" or the "International Branch");

WHEREAS, Nordea helped its customers set up hundreds of offshore accounts for tax-sheltered companies, including companies connected to the Panama Papers data leak;

WHEREAS, Nordea, through its Baltic operations, has been linked to billions of dollars of high-risk transactions, including certain transactions connected with money laundering, and transactions involving parties associated with financial crime;

WHEREAS, Nordic financial regulatory authorities, including the Danish Financial Supervisory Authority ("D-FSA"), the Finnish Financial Supervisory Authority ("FIN-FSA"), the Swedish Financial Supervisory Authority ("S-FSA"), and the Norwegian Financial Supervisory Authority (the "N-FSA") have previously identified weaknesses in Nordea's Anti-Money Laundering ("AML") compliance programs and other compliance deficiencies;

WHEREAS, the Department has been investigating various aspects of Nordea's operations, including whether the Bank violated New York law by allowing compliance deficiencies to persist in its Bank Secrecy Act/Anti-Money Laundering program and procedures;

WHEREAS, the Department's investigation has focused on the adequacy of Nordea's AML program in its Baltic Branches and the International Branch, its AML controls over its correspondent banking relationships, and its transaction monitoring system; and

WHEREAS, the Department has found that Nordea's AML program in its Baltic Branches and the International Branch was deficient; that Nordea failed to adequately conduct

due diligence on its correspondent banks; and that Nordea's transaction monitoring system was inadequate.

NOW THEREFORE, to resolve this matter without further proceedings pursuant to the Superintendent's authority under Banking Law §§ 39 and 44, the Department finds as follows:

THE DEPARTMENT'S FINDINGS FOLLOWING INVESTIGATION

Introduction

1. Global financial institutions serve as bulwarks against illegal financial transactions in today's interconnected financial world.

2. The federal Bank Secrecy Act (the "BSA") mandates that financial institutions implement adequate AML policies and systems in their operations to prevent illicit financial transactions from occurring. New York State law requires financial institutions to maintain systems reasonably designed to identify and report suspicious activity and block transactions prohibited by law. All regulated institutions are expected to configure protective systems that are aligned with the AML risk factors unique to them and must ensure that these systems run effectively.

3. Financial institutions must also monitor their customers and their customers' transactions to ensure that there is no nexus to, or facilitation of, criminal activity. Accordingly, know your customer ("KYC"), customer due diligence ("CDD"), and Counter Terrorist Financing ("CTF") procedures are paramount in the maintenance of effective AML controls. For customer relationships that pose an especially high risk, financial institutions should conduct more frequent ongoing due diligence ("ODD") and enhanced due diligence ("EDD").

4. In certain instances, however, even ODD and EDD measures may be insufficient. If the money laundering risks posed by a particular customer relationship are too elevated to be contained, then the financial institution should consider terminating the relationship.

5. Financial institutions must also perform KYC and CDD on their relationship banks, i.e., banks with whom they maintain correspondent banking relationships or exchange Society for Worldwide Interbank Financial Telecommunication ("SWIFT") relationship management application ("RMA") keys. In these reviews, banks must assess if the existence of a relationship with another bank poses too great a risk to be mitigated by diligence measures and, if so, should consider terminating the relationship.

6. Financial institutions are increasingly intertwined, maintaining relationships with many other financial institutions that provide them with access to financial systems far beyond their various borders and local geographies. These relationships are formed in order to facilitate financial transactions in a wide range of currencies. Financial institutions need to be wary, however, of forming relationships with other institutions domiciled in countries that pose heightened money laundering risks, and with banks whose governance structures and inadequate internal controls leave them exposed to elevated money laundering risks.

7. In addition, financial institutions must maintain transaction monitoring programs, which are critical for monitoring transactions for Money Laundering/Terrorist Financing ("ML/TF") violations and suspicious activity reporting. Such systems allow financial institutions to maintain awareness over transactional patterns in order to identify transactions that are suspicious based on empirical typologies and scenarios that conform with known ML/TF methods. A financial institution's transaction monitoring program must be routinely updated to ensure its continued efficacy.

8. For the reasons set forth more fully below, the Department has determined that Nordea failed in various respects to meet these obligations with respect to its AML program and procedures at the Baltic Branches and the International Branch, due diligence procedures with respect to its correspondent bank and other customer relationships, and transaction monitoring. Nordea has acknowledged its shortcomings in these respects to the Department.

Nordea's Operations

9. Nordea, a global financial institution, is the largest bank in the Nordics and one of the largest corporations in the Nordic region. As of 2023, Nordea's total assets were worth approximately $627 billion, and its New York Branch had more than $37 billion in assets. From 2000 through 2017, Nordea had branches in Estonia, Latvia, and Lithuania, as well as an international branch in Vesterport, Denmark. Nordea maintains a Group back-office function in Estonia, which is focused on supporting certain operations in the Bank.

Investigation Regarding Entities Associated with Money Laundering Activities

10. In April 2016, around 11.5 million records were leaked from the Panamanian law firm, Mossack Fonseca & Co. The files exposed, among other things, offshore companies controlled by members of royal families and political leaders, and the hidden financial dealings of politicians and public officials. Most importantly, the leak showed the failure of financial institutions around the world to follow legal requirements that would ensure their customers were not involved in criminal endeavors, tax evasion, or political misconduct. Nordea was one of the financial institutions implicated.

Nordea's Baltic Branches

11. With the fall of the Soviet Union in 1991, the fast-growing Baltic countries Estonia, Latvia, and Lithuania, became attractive markets for Nordic companies, who increased

their business activities there. Nordea viewed the Baltics as a natural extension of its Nordic home market, establishing a presence in those countries as part of its long-term growth strategy. Nordea would go on to describe itself as having "the largest customer base of any bank in the Nordic and Baltic region."

12. In 1995, Nordea established its Estonian Branch. In 1999, Nordea commenced its operations in Latvia by becoming the sole shareholder of a Latvian Bank. In 2000, Nordea opened its Lithuanian Branch.

The Money Laundering Risks in the Baltics

13. With this potential for growth, however, also came the potential for great risk. Nordea would later acknowledge in its risk assessments the risks posed by potential money laundering in the Baltics. Nordea observed that "[c]ustomers from post-Soviet countries with [a] high corruption index . . . increases the risk of a bank in Estonia being used for ML [money laundering]." Operating in Latvia presented similar risks, with Nordea again observing that, "the main threats" facing Nordea Latvia "are connected with money laundering." Features unique to Latvia that made it vulnerable to such threats included "[t]he large extent of a 'shadow' economy" and the geographic location of the country as "a bridge between the economies of Russia and the other post-Soviet states and Europe and the world's financial systems." Nordea identified similar concerns in its risk assessment for its Lithuanian Branch.

Deficiencies in Nordea's Anti-Money Laundering Controls and KYC in its Baltic Branches

14. Many of the issues Nordea first identified in 2010 persisted into 2017. Although Nordea made certain improvements to its AML compliance program, it was slow to remediate the many issues flagged by its own audit committees.

15. In 2010, Nordea employed a new Group KYC Directive which set KYC policy and processes throughout its entire operations, including at the Baltic Branches. The directive required a risk-based approach to KYC compliance, with the level of KYC tailored to the risk level of the customer. CDD was required before any customer relationship could be established, with EDD a requirement for higher risk clients and Simplified Due Diligence ("SDD") acceptable for certain lower-risk entities.

16. In 2010, Nordea's Group Internal Audit ("GIA") assessed the Baltic Branches against new Group AML/CTF and KYC directives and instructions, introduced in mid-2009. While the audit acknowledged steps taken at the Baltic Branches to reflect and respond to the new requirements, it identified shortcomings in the AML systems in place at the branches. The audit found a lack of soundness in AML and KYC standards stemming from an overreliance on manual monitoring. The audit acknowledged that IT development projects were underway to address this issue but was concerned that "the Baltic Branches [had] limited possibilities to affect" such IT processes. The audit also included a sample-based review of the Baltic Branches' customer identification data, and "observed shortcomings in 50% of the cases." These shortcomings led to weaknesses in AML, CTF and KYC controls in the Baltic Branches.

17. In 2012, Nordea conducted a gap analysis to assess gaps between AML processes and compliance in its Baltic Branches as compared to Finnish AML standards and FIN-FSA requirements, finding several areas to be remediated. One gap identified related to the identification of Politically Exposed Persons ("PEPs"). This gap was traced to the Baltic Branches' adherence to the less stringent standards in Baltic legislation regarding PEP identification; however, shortcomings in the Baltic Branches' approach to PEP identification would persist due to a lack of automatic customer PEP screening and problems with the

functionality of PEP screening systems. Another gap identified across the Baltic Branches concerned the FIN-FSA requirement to identify persons or transactions from sanctioned countries, or countries with insufficient AML controls. The FIN-FSA requirement to regularly update customer information was also identified as a gap at the Baltic Branches.

18. Recognizing that AML standards imposed by Baltic regulators at times fell short of FIN-FSA requirements, Nordea updated its Group KYC standards in June of 2012, requiring its Group standards to be applied in the Baltics even when national legislation in the Baltics was less stringent. Furthermore, where national legislation was more stringent than Nordea Group requirements, the Group Directive set forth that local requirements would take precedence. Nevertheless, Nordea's Baltic Branches fell short of full compliance with the Group Directive.

19. In 2014, Nordea's GIA measured compliance with the 2012 Group Directive and rated the Baltic Branches with an "Improvements Needed" rating for "Customer Due Diligence." More specifically, at the Estonian Branch, GIA identified shortcomings in the CDD performed on some corporate customers, including missing information on the origin of the funds and the line of business in which corporate customers were involved. At the Latvian Branch, the audit uncovered instances where "not all necessary information was filled in[to] the customer questionnaires." Finally, at the Lithuanian Branch, the audit described how, while CDD processes were in place, "they were not always thoroughly completed up to group and/or local requirements." The audit acknowledged that some differences between Group and Baltic Branch processes at this time were a result of different requirements under Baltic law. Other differences in CDD practices stemmed from shortcomings in the application of Group CDD requirements at the Baltic Branches even when such requirements were incorporated into local written procedures.

20. Similarly, regarding EDD at the Baltic Branches, the 2014 audit observed that while EDD procedures were in place across all branches, there were shortcomings in adherence to the 2012 Group Directive. Those shortcomings varied between Baltic Branches but included the lack of EDD-specific forms at the Estonian and Latvian Branches, and insufficient EDD measures for high-risk customers, including foreign PEPs, as well as failures to conduct necessary diligence measures such as requesting a customer's former relations with other financial institutions and requiring bank references. The 2014 audit also flagged deficiencies in the Baltic Branches' approach to their Customer Risk Rating methodology, the manual nature of the process, and the lack of specific risk rating documents to aid in its manual application. Deficiencies in relation to AML training for Baltic Branch employees were also observed.

21. In April 2016, Nordea's Group Business Risk Implementation and Support ("BRIS") unit, together with each respective Baltic Branch's Group AML and Sanctions unit, carried out ML/TF risk assessments for each of the each of the Baltic Branches. While some improvements were noted, many of the problems with AML controls in the Baltic Branches persisted.

22. At the Estonian Branch, the 2016 Risk Assessment once again found "low data quality due to insufficient KYC data," specifically that "28% of active Household" customers "have outdated or insufficient KYC data." The Risk Assessment acknowledged that the introduction of an "IT supported tool to gather KYC information" for CDD had decreased previously identified risks, and that the quality of KYC update reporting had improved, but also that the practice of manual risk scoring increased the risk of operational mistakes. The Risk Assessment also identified that implementation of Nordea's Group policies at the Estonian Branch was again incomplete, the Group High Risk Country list was not implemented, the Group

High Risk Industry list was not implemented, and the Group AML Risk Scoring model was insufficiently implemented.

23. AML procedures and resources were found to be lacking. The assessment noted that "[f]ormal written procedures [were] not in place for several areas." In addition, "[t]oo few resources [were] allocated on AML/CTF and Sanctions", and there were "[t]oo few SAR reports" filed with the relevant authorities "compared to benchmark in [the] Financial Industry in Estonia." The Risk Assessment nonetheless acknowledged some improvements such as an increase in the staffing of the Baltic Group AML and Sanctions unit.

24. The Risk Assessment found that ODD processes were not fully implemented at the Estonian Branch, and EDD processes, while implemented, were not fully functional. As found in prior years' audits, the Estonian Branch's continued reliance on manual processes and lack of IT-supported diligence tools presented an AML compliance risk.

25. At the Latvian Branch, the 2016 Risk Assessment observed problems with KYC data finding, "[o]utdated and/or insufficient KYC information on [approximately] 36% of Corporate customers and 22% of Household customers." The incomplete data meant the Latvian Branch did not know its customers sufficiently thus exposing it to increased AML risk.

26. Regarding CDD, ODD, and EDD, the Risk Assessment noted comprehensive IT-supported tools, processes, or quality control features were not fully in place. More generally, "[f]ormal written procedures are missing/lacking in several risk areas." In connection with this, the Risk Assessment noted that a new EDD process implemented in Q1 2016 would serve to decrease the risks at the Latvian Branch. Further, high limits for cash deposits and insufficient controls in this area added to the Latvian Branch's risk level. The assessment further found

"[t]oo few resources allocated on AML/CTF and Sanctions," but noted that additional resources had been "approved" in this area.

27. Nordea's Group-wide policies were not fully implemented at the Latvian Branch. Nordea's Group Scoring model was found to be insufficiently implemented and the existing manual risk scoring did not include all relevant risk factors. Furthermore, neither Nordea's Group High Risk Country nor its High-Risk Industry lists were implemented at the Latvian Branch (though a high-risk industry list issued by the local financial supervisory authority was used). And while non-resident customers accounted for 2% of the customer base, they held 10% of all deposits.

28. Similar shortcomings with KYC and AML processes were also observed at the Lithuanian Branch. The Risk Assessment noted low data quality due to insufficient KYC and too few resources allocated to AML/CTF controls. Additionally, AML/CTF awareness was found to not be properly incorporated in the business processes; and comprehensive IT tools to support proper EDD, ODD, and CDD were not sufficiently implemented. The risks presented by the Lithuanian Branch's KYC and AML deficiencies were exacerbated by the high level of risk in its customer base, with the Risk Assessment finding "[r]elatively large amount[s] of customers with a link to High Risk countries with high corruption index which increases the risk of Nordea being used for ML [money laundering]."

29. In sum, throughout 2010 to 2016, there were deficiencies in the AML and KYC processes at the Baltic Branches. While the Bank undertook remedial steps and made improvements to its AML compliance program, many of the issues first flagged by its own audit committees in 2010 persisted into 2017.

Nordea's Baltic Branches' Transition to Luminor

30. On August 25, 2016, Nordea and the Norwegian bank Den Norske Bank ("DNB") entered into an agreement to combine their operations in Estonia, Latvia, and Lithuania to form an independent financial services provider in the Baltics. On October 1, 2017, the transaction was successfully closed, and the combined entities were renamed Luminor Group AB ("Luminor"). Luminor comprised approximately 930,000 of DNB's former customers and 350,000 of Nordea's former customers. Under the terms of the merger deal, Nordea initially retained 56.5% of the economic rights and 50% of the voting rights of Luminor, and DNB held 43.5% of Luminor's economic rights.

31. The Nordea-Luminor relationship was governed by Transitional Services Agreements ("TSAs"). Under the TSAs, all Luminor domestic transactions and certain Luminor international transactions would be processed through Nordea Finland, and Luminor would receive access to Nordea's correspondent banking network. These arrangements exposed Nordea to certain of Luminor's risks, both in terms of credit exposure and financial crimes risk.

32. Within Nordea, the International Banks unit ("IB"), the division that oversaw Nordea's correspondent banks, became the Customer Responsible Unit ("CRU") for Luminor. IB maintained an AML oversight role over Luminor, and according to a Nordea memorandum, became "accountable for the relationship in terms of credit exposure and financial crime risk." Under the TSAs, Nordea undertook "to apply AML/CTF due diligence measures" on behalf of Luminor, receiving fees in return. Nordea also agreed to provide Luminor access to its Transaction Monitoring system, specifically the Financial Anti-Crime Platform ("FACP"), and to investigate alerts generated by FACP.

33. Nordea was concerned about the risk posed by its relationship with Luminor. Certain IB personnel suggested at the time that they were "not comfortable with [the] risk of Luminor" in light of "red flags" identified in Luminor's operations. These included: Luminor's SWIFT payment counterparty data being in noncompliance with international correspondent banking industry standards; gaps in Luminor's data; Luminor's high-risk customer base, including money service businesses; and Luminor's limited understanding of red flags and the actual purpose and nature of its customer relationships. IB personnel observed that they "[could not] apply mitigating and legally required controls such as sanctions screening and transaction monitoring," owing to Luminor's poor data.

34. Certain Nordea employees were especially alarmed that Luminor customers maintained direct access to Nordea's web-based banking platforms, including its online corporate banking platform, "in the same manner as if they were Nordea customers." This was particularly troubling because there was "no CRU appointed in Nordea for Luminor customers that maintain access to Nordea platforms," and there was "no appointed team for handling escalations of sanctions screening alerts" for Luminor customers who used Nordea's platforms.

35. Luminor customers' access to Nordea's banking systems was characterized in an email by a Nordea financial crime specialist as "a severe breach of at least (but not limited to) information security rules, financial crime regulatory frameworks and an incident report must be filed immediately." The specialist wondered, "[h]ow is it possible that Luminor has access to our legacy systems?"

36. The heightened risks posed by the Nordea-Luminor relationship negatively impacted Nordea's relationships with its U.S. dollar-clearing banks. Nordea noted a continuing uptick in inquiries from its dollar clearing bank in the Baltics about Luminor's customers and

their transactions, and received rejections for Luminor U.S. dollar payments from certain other U.S. financial institutions. Nordea resolved to adequately respond to the inquiries from its dollar clearers so that it could maintain these relationships.

37. Between 2007 and 2019, Nordea's primary U.S. dollar clearing bank in the Baltics processed 553,886 U.S. dollar transactions with Nordea Bank Abp worth approximately $119.7 billon. Between 2007 and 2017, Nordea's primary U.S. dollar clearing bank processed approximately 325,000 U.S. dollar transactions with the Lithuanian Branch worth approximately $74.7 billion. Following the formation of Luminor, Nordea's Lithuanian Branch's U.S. dollar correspondent account with its primary U.S. dollar clearing bank was reassigned to Luminor. Between 2018 and 2019, 69,742 U.S. dollar transactions involving Luminor worth approximately $3.2 billion were processed through this account.

38. In December 2017, Nordea and Luminor undertook a joint remediation project dubbed "Project Lux." Commendably, Project Lux focused on remediating KYC deficiencies at Luminor, improving its transaction monitoring program, and enhancing its overall financial crime control framework. Nordea held numerous Project Lux steering group meetings together with Luminor.

39. However, serious AML risks in the Nordea-Luminor relationship persisted, as described in subsequent Project Lux steering group meetings. At one such meeting, Nordea expressed concern that because "[a]ll domestic Luminor transactions flow[ed] through Nordea Finland" Nordea could be liable for AML and sanctions screening violations associated with these transactions, which were not at the time screened or monitored by Nordea. Further, "Luminor international transactions flowing through Nordea's systems [were] only being

partially monitored," thus exposing Nordea to AML risk in U.S. dollar and other currency transactions.

Nordea's International Branch at Vesterport Denmark

Background Information on Nordea's Vesterport Branch

40. In 1989, Nordea opened the International Branch ("VIB" or "the International Branch"), as part of the Bank's Cash Management function, in Vesterport, Denmark. In 2003, VIB became a part of Retail Banking in Denmark. VIB served corporate customers, including companies registered or owned outside of Denmark. By 2013, approximately 55% of Nordea Denmark's corporate customers with foreign addresses were being serviced by VIB. VIB's corporate customers were principally commercial or manufacturing companies that needed international cash management services. As a matter of general policy, VIB did not open accounts for financial companies (e.g., investment companies, broker companies, holding companies or companies with bearer shares). VIB broadly categorized its customers as either "West" or "East" customers depending on their country of organization.

41. VIB's West customers included companies with strong connections to Denmark or other Nordic markets, or companies referred by Nordea's other branches in the Nordics or Western Europe. VIB's East customers typically were companies registered or incorporated outside of their home nations and acted as intermediaries to commercial and manufacturing enterprises that were in, or beneficially owned by persons in, Russia and Eastern Europe. By 2014, East customers accounted for approximately one-half to two-thirds of the total VIB customers (i.e., approximately 1,500 customers). More than a third of VIB's customers were onboarded prior to 2009.

42. This group of East customers would ultimately expose VIB to numerous money-laundering scandals, including the Panama Papers, the Russian Laundromat,[1] the Azerbaijani Laundromat,[2] and the Hermitage Capital Allegations.[3] Seventy-two VIB customers were identified as connected to the Panama Papers scandal. In connection with the Russian Laundromat, twenty-nine customers of VIB were counterparties to Moldindconbank and Trasta. These were all subject to suspicious activity reports by Nordea to local regulators. Nine Nordea customers were counterparties to the four subjects named in the media reports related to the Azerbaijani Laundromat, and of the nine, one was an inactive VIB customer. Eleven customers of VIB were connected to the Hermitage Capital Allegations. Similarly, these were all subject to suspicious activity reports by Nordea to local regulators.

AML Compliance Deficiencies at VIB

43. While the Bank's, including VIB's, overall AML program developed and evolved over time, an AML audit from 2009 identified that weaknesses in CDD and monitoring were present as early as 2009.

44. Beginning in mid-2013, there was an increase in correspondent bank inquiries concerning VIB customers. That same year an internal review identified some improvements in customer due diligence procedures, but also revealed significant gaps in VIB procedures in meeting new KYC standards. These included failures to obtain documented verification of

[1] The Russian Laundromat was a scheme that laundered an estimated $20 billion from Russian shell companies into banks throughout the European Union and around the world between 2010 and 2014. Two of the banks involved in the scheme were Moldindconbank of Moldova, and Trasta Komercbanka of Latvia.
[2] The Azerbaijani Laundromat was a scheme that laundered over $2 billion between 2012 and 2014 through four UK registered shell companies.
[3] In 2018, Nordic authorities received a complaint from Hermitage Capital Management that $175 million in illicit funds had flowed through Danske Bank's branch in Estonia, and Ukio Bankas in Lithuania into hundreds of accounts at Nordea.

expected transactions from customers' accounts, including volume, origin, source of funds, and identification of corporate representatives.

45. An October 2013 Group Internal Audit found gaps in the EDD process for a sample of 10 VIB customer files, including failures to record the beneficial owners in the Bank's Customer Information Control System ("CICS") database for two customers, failures to record two customers as high risk in the database, and failures to include the origin of funds on the EDD checklist for onboarding, which led to incomplete EDD for certain customers. While VIB undertook remediation efforts following the 2013 audits, including, for example, conducting a review of all customers (East and West) onboarded between 2009 and 2011, there were elements of the 2013 audit that remained unresolved until the International Branch's closure in 2014.

Rerouting of Funds and Failures to Block Certain Transactions at VIB

46. Beginning in 2013, the media began to question Nordea's facilitation of business in offshore tax havens. The reports specifically alleged that the VIB did not investigate the ownership of offshore customers who made payments through the bank through professional agents.

47. Additionally, in late 2013, the International Branch encountered an increase in correspondent bank inquiries, rejected payments, and stop requests. Nordea experienced an increase in inquiries received concerning VIB customers into 2014.

48. In response to the correspondent bank inquiries, rejected payments, and stop requests, VIB personnel re-routed three blocked transactions.

49. By way of example, in January 2014, a U.S. bank informed VIB of rejected payments involving a customer of the VIB branch that had been resubmitted by another VIB customer with the same beneficial owner. These payments were rejected by the U.S. bank

between August and September 2013 due to concerns related to negative press, and internal discussions at the U.S. bank. This issue led to the Bank identifying a "hole" in the payment system that allowed a customer to change the name of the sender, which made the ordering customer information inconsistent with the account number. At that time, the relationship managers at Nordea would focus their review on the purpose of the payment, as opposed to the customer's name or beneficial owner, and since the purpose of this transaction was consistent with previous transactions, the managers failed to make a connection between those payments and the ones rejected.

50. In a separate matter in early 2014, VIB personnel discussed the possibility of re-routing funds for a customer who was the subject of a cease-and-desist request from another U.S. bank. This customer sent a payment to an individual who was added to the OFAC sanctions list after the transaction was completed. Before a VIB working group established to address issues related to blocked payments could come to a consensus as to whether payments should be re-routed after conducting EDD, Nordea personnel rerouted this payment.

51. Another example occurred in June 2014, when a U.S. bank issued a cease and desist for a VIB customer due to the "shell like nature" of the activity. A task force was created within VIB, and after performing EDD, VIB re-routed the payments while it waited for confirmations from the customer.

52. The U.S. bank issued a second cease and desist request to VIB for another customer that same month. The task force thereafter determined that the relationship with the customer needed to be terminated, along with other customers with the same beneficial owner, and further determined that EDD had been conducted without all necessary information having been received.

53. While the Bank established a task force to address these incidents and ensure proper remediation for rejected payments and cease and desist orders, Nordea lacked a standardized approach to responding to requests regarding EDD and cease and desists. Specifically, in 2013 and early 2014 there were no procedures to block payments from certain customers from correspondent banks or to prevent the re-routing of payments to other correspondent banks.

The Closure of VIB

54. In early 2014, during the Russian invasion of Ukraine and subsequent annexation of Crimea, the Bank grew concerned with monitoring new sanctions related to its VIB East customers.

55. The implementation of new U.S. sanctions created a need to revisit all the East customers onboarded before 2009. In March 2014, there were approximately 800 East customers for whom VIB had not obtained or registered complete beneficial owner information. Compliance personnel expressed concern that VIB was at risk for noncompliance due to the substantial number of Ukraine- and Russia-connected VIB customers. As an interim solution, VIB conducted manual screening of payments to Ukraine and a task force was established to address the risk.

56. In April 2014, due to an increase in correspondent bank inquiries and requests, the Branch stopped onboarding East customers. In June 2014, the CEO of Nordea Denmark informed members of the Group Executive Management team, and the Deputy Head of Banking Denmark, that he had decided to close VIB, and about 1,800 customer accounts were exited or scheduled to be exited in 2014. VIB faced challenges in carrying out the exiting process,

including uncooperative and unresponsive customers. This led to a delay in the terminations, causing them to be carried into 2015.

57. The forced termination of accounts caused East customers to seek to open accounts in Nordea's Baltic Branches, and Luxembourg. This posed further complications for Nordea as it was unable to monitor whether exited customers were onboarded at other branches of the Bank, due to bank secrecy restrictions limiting the sharing of customer information across branches.

58. VIB was primarily closed in 2014, while the last of the offboarding occurred in 2015. Retained customers were managed under the Copenhagen region of Retail Banking until 2016.

Nordea's Correspondent Banking and RMA Relationships

Background Information on Nordea's Correspondent Banking and RMA Relationships

59. Nordea maintained correspondent banking relationships with various financial institutions. Nordea also exchanged numerous SWIFT RMA keys with financial institutions. RMA is a filter that is mandated by SWIFT which allows financial institutions to decide which counterparties are able to send financial information ("FIN") messages. This gives financial institutions the ability to block unwanted messages and allow others. The Department has concluded that Nordea failed to adequately monitor and manage its correspondent and RMA relationships, particularly with Danske Bank, ABLV, and Bank of Cyprus.

60. In 2012, after a FIN-FSA inspection, the Bank shifted from country-based risk assessments to bank-specific KYC assessments, which assigned risk classes to its correspondent banks.[4]

61. In 2015 and 2016, the Swedish Financial Authority ("S-FSA") and the Danish Financial Authority ("D-FSA") conducted investigations into Nordea's AML compliance program, transaction monitoring program, and correspondent banking relationships. Both regulators identified issues related to the implementation of internal policies, employee training, and the lack of uniform guidelines.

62. A 2015 Group Internal Audit of AML and CTF in Correspondent Banking Relationships scored Nordea an overall "critical" rating. At that time, Nordea did not have formal agreements with all of its correspondent banks on AML responsibilities; did not have adequate instructions for conducting customer due diligence, as the instructions were not specifically "designed to assess and remediate the specific customer type risk"; did not provide sufficient training for its employees on the correspondent banking guidelines; failed to perform EDD at a more enhanced level than standard diligence for its high-risk correspondent banks; and did not fully fill out its ODD forms.

63. The audit also found that there were banks that had open RMA keys with Nordea and were not listed in Nordea's CDD-approved correspondent banking network. GIA feared that this meant that Nordea was maintaining relationships with banks previously marked for exit and was not performing sufficient diligence or transaction monitoring measures on banks that may have had poor AML/CTF controls.

[4] Correspondent banks assigned to risk class "A" were reviewed every three years, correspondent banks assigned to risk class "B" were reviewed every two years, and correspondent banks assigned to risk classes "C" and "D" were reviewed annually. Correspondent banks assigned to risk classes "B" through "D" were also subject to EDD.

64. In response to risks identified in the 2015 Group Internal Audit, Nordea initiated an AML review of correspondent banking, which was referred to as the Correspondent Banking, GIA Project. Nordea also prepared an action plan for remediation, which included implementing higher standards for KYC/AML guidelines for International Banks, enhancements to the due diligence process, and the recruitment of KYC/AML experts.

65. Additionally, prior to 2017, Nordea only collected KYC and CDD information at the Group or parent level of its correspondent banks as opposed to the branch level. In an effort to enhance its KYC processes, Nordea changed its KYC and CDD collection process in 2017 and began collecting KYC and CDD information from correspondent banks at the branch level.

66. The Bank's efforts between 2012 and 2018 to improve correspondent banking related policies and procedures coincided with a correspondent banking network reduction project, which was designed to reduce the risks posed by certain correspondent banking relationships. By 2013 the project had led to a 50% reduction in the Bank's correspondent banking network. This was further reduced by ~50% in 2017, and by ~13% in 2023.

Nordea's Correspondent Banking Relationship with Danske Bank

Background

67. Danske Bank ("Danske") is headquartered in Copenhagen, Denmark, and is one of the largest banks in the Nordic region. Nordea and Danske have substantial relationships spanning numerous markets. Annual cross-border payment traffic between the two banks in U.S. dollars was about $100 billion.

68. Although Nordea did not provide U.S. dollar correspondent accounts for Danske, it did provide Norwegian Krone ("NOK") and Euro ("EUR") correspondent accounts to Danske's Danish Entity. Nordea's NOK and EUR accounts were closed in 2015 and 2016,

respectively, but Nordea continues to provide a Swedish krona ("SEK") correspondent account to Danske's Danish entity and continues to maintain open RMA keys with Danske.

69. In 2007, Danske acquired Sampo Bank in Finland and various subsidiaries in the Baltics, which included an Estonian bank, which became known as Danske Bank Estonia ("Danske Estonia"). Nordea did not provide correspondent accounts to Danske Estonia, but Danske Estonia maintained RMA keys with various Nordea locations from 2008 through 2019. Danske Estonia operated from 2008 until its closure in 2019.

Nordea's Deficient KYC on Danske Bank

70. Nordea did not collect KYC on Danske Estonia until 2017, because before 2017 the Bank only collected KYC information at the Group level.

71. In 2013, Nordea granted Danske KYC approval with an AML risk class "A" rating. Nordea rated Danske in risk class "A" rating, despite Danske having been issued an adverse decision by the D-FSA in 2012 for deficiencies in correspondent banking and customer identification purposes. That 2012 decision cited to deficiencies in Danske's cross-border correspondent banking and customer identification processes. A subsequent D-FSA decision issued later the same year found that Danske had complied with all the administrative orders expressed in the previous decision and "reacted appropriately to [D-FSA's] risk mitigation recommendations."

72. In 2015, the D-FSA's inspection of Danske Bank found that Danske had in fact violated correspondent bank provisions of the Danish AML Act and had failed to comply with the D-FSA's 2012 order. As a result, the D-FSA made a criminal referral to Danish law enforcement. The criminal referral led the Bank to conduct an event-driven review of KYC on Danske in early 2016.

73. As part of this KYC update, Nordea created a "CDD/EDD Matrix," designed to cover various data points, including Danske's products, customers, and risk management controls. The CDD/EDD Matrix revealed deficiencies in Danske's AML Program, particularly regarding its correspondent banking due diligence program, and its exposure to potential money laundering risks at Danske Estonia, which were not properly addressed.

74. After a Compliance Meeting in 2016 where Danske informed Nordea of the controls implemented in response to the D-FSA findings, and its intent to only keep corporate customers with a Nordic link at Danske Estonia, Nordea assigned Danske an AML risk class "C" rating in recognition of the heightened risks posed by the bank and the commensurate need to apply heightened monitoring and oversight to the relationship. Danske continued to receive an AML risk class "C" rating in 2017 and 2018.

75. In both the 2017 and 2018 KYC reviews, Nordea pointed to negative news concerning Danske and Danske Estonia, but also cited to "some good comforting factors which we consider to be enough to mitigate identified risk factor[s]".

76. In September 2017, Nordea created an internal task force to review Danske Estonia's relationship with Nordea and the Azerbaijani Laundromat. Danske informed Nordea that the possible exposure issues were related to Danske's 3,000 to 4,000 non-resident customers, primarily from Russia and other former Soviet Union nations.

77. By only collecting KYC at the Group level, Nordea was unable to be fully aware of Danske Estonia's involvement and activities in money laundering schemes.

78. In 2017, Nordea rated Danske Estonia an AML risk class "C" rating and, by October 2019, eight months after a precept was issued by the Estonian Financial Supervisory Authority, Danske Estonia ceased its activities.

Nordea's Internal Reviews of Danske Estonia

79. Four entities that were central to the Azerbaijani Laundromat were customers of Danske Estonia. Nordea conducted a review of these four entities and identified nine Nordea customers as payment counterparties, though one was an inactive VIB customer.

80. In September 2018, the Bank conducted a review regarding its potential exposure to Danske Estonia in connection with reports of around €200 billion of suspicious funds connected to Danske Estonia's non-resident portfolio that may have been transacted through Danske Estonia from 2007 until 2015. The Bank identified 341 customers, associated with red-flagged transactions, as high-risk. Of the 341 customers, 104 were active customers, and 76 of the 104 had not been reviewed in previous internal investigations.

81. After the Hermitage Capital Complaint, Nordea initiated a review targeting the transactions mentioned in the Complaint. The New York Branch also initiated a preliminary search of transactions between the New York Branch and Danske Estonia, which identified 67 transactions totaling $5.1 million involving Danske Estonia, between 2008-2019.

82. From 2011 to 2015, Nordea identified 16,863 payments between Danske Bank Estonia and Nordea's Head Office and its New York Branch. Of the 16,863 payments, accounting for approximately $1.8 billion, 76 payments were processed through the New York Branch. High-risk parties were identified in 479 of the payments, with the total value of their payments totaling approximately $84.5 million.

Nordea's Correspondent Banking Relationships with ABLV

83. Founded in 1993 and headquartered in Riga, Latvia, ABLV Bank ("ABLV") was one of the largest private banks in the Baltic region. In February 2018, the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") issued findings naming

ABLV an institution of primary money laundering concern, along with an accompanying notice of proposed rulemaking ("NPRM") pursuant to Section 311 of the PATRIOT Act. In its NPRM, FinCEN found that "ABLV's management permits the bank and its employees to orchestrate money laundering schemes, solicits high-risk shell company activity that enables the bank and its customers to launder funds, maintains inadequate controls over high-risk shell company accounts, and seeks to obstruct enforcement of Latvian anti-money laundering and combating the financing of terrorism (AML/CFT) rules in order to protect these business practices." Nordea terminated its correspondent banking relationships with ABLV shortly after FinCEN's determination.

84. Between 1996 and 2015 Nordea provided a U.S. dollar correspondent account to ABLV's Latvian head office, ultimately closing the account in response to increasing compliance inquiries from other banks. Between 2008 and 2018, Nordea entities in Denmark, Norway, Sweden, and Finland provided correspondent accounts to ABLV in Danish Krone, Norwegian Krone, Swedish Krona, and Euros. ABLV also exchanged RMA keys with 12 Nordea locations between 2008 and 2018. Between 2010 and 2014 Nordea's head office processed 22,487 U.S. dollar transactions involving ABLV worth over $17.7 billion. Between 2010 and 2018, Nordea's New York branch and ABLV engaged in approximately 457 U.S. dollar transactions worth approximately $293 million.

Nordea Performed Insufficient Customer Due Diligence on ABLV and Delayed Terminating this Relationship Notwithstanding Numerous Red Flags

85. Nordea's 2018 termination of its correspondent banking relationships with ABLV came too late. It was evident from Nordea's ABLV KYC diligence materials between 2014 and 2018 that the Bank identified a number of concerns regarding the risks posed by the ABLV relationship.

86. In 2013, Nordea assigned ABLV an AML risk class "B" rating. According to Nordea's policy, banks in risk class B would be subject to an annual ODD review. Overall, Nordea was pleased with ABLV's AML/CTF controls, noting that "[n]o PEPs have been found"; "[t]he bank has a good process and good policies in place"; and "[w]e have met with the bank in Latvia in November 2013 and we have a good dialog with them." One year later, however, the tenor of Nordea's annual ODD review of ABLV changed. The Bank observed that annual ODD was no longer sufficient, but rather "[q]uarterly ODD is recommended due to the present situation in Russia and the discussion on the possibility of money laundering through Latvia." Mistakenly, however, the 2014 ODD form failed to include this recommendation in its conclusions section, writing instead that "[n]o further action [was] required -- as no triggers were identified based on above ODD." As a result, remediation measures that were crucial for the containment of AML risks associated with ABLV were delayed in their implementation.

87. Nordea's 2015 KYC file on ABLV reflected the Bank's increased concerns regarding ABLV's AML controls, leading Nordea to downgrade ABLV to AML risk class "C". One of Nordea's concerns related to ABLV's high geographic and customer risks stemming from its branches in high-risk jurisdictions such as Russia, Ukraine, and Azerbaijan. Another concern pertained to allegations of money laundering activities occurring through ABLV bank accounts.

88. In light of those concerns, Nordea informed ABLV that it would be closing ABLV's USD account on February 20, 2015. ABLV asked Nordea to reconsider and provided Nordea with a presentation and various assurances regarding its AML compliance program. However, Nordea reiterated its decision to ABLV on March 2, 2015, and closed the USD account on April 7, 2015.

89. Nordea's concerns with ABLV's AML controls persisted into 2016, resulting in Nordea again assigning ABLV to AML risk class "C." Nordea observed that ABLV had a subsidiary in Russia; that ABLV employees did not perform customer identification and certain AML and CTF functions, with these roles outsourced to third parties; that ABLV customers were engaged in high-risk cash-intensive businesses, such as gambling and arms dealing; that ABLV was fined by its local regulator, for, *inter alia*, having "not performed initial customer due diligence before launching business relations"; that ABLV's shares were not listed on a regulated market; and that ABLV "offers downstreaming to several smaller Russian banks and this poses a higher AML risk." Notwithstanding these risks, Nordea elected to maintain its correspondent banking relationship with ABLV. However, Nordea foreshadowed that after the planned merger of its Baltic entities with DNB, it would reconsider and "evaluate if this bank should remain in our network."

90. In December 2016, reporting from the Organized Crime and Corruption Reporting Project ("OCCRP") regarding money laundering in Baltic banks, including at ABLV, raised further red flags within Nordea and triggered event-driven EDD. In January 2017, Nordea's Relationship Manager ("RM") for ABLV, in reaction to the December 2016 OCCRP report, wrote in an email that their "conclusion is that ABLV has been the receiver of dirty money hence you would question their AML/KYC procedure and their ability to act according to these." The RM added that it would be important as part of Nordea's future EDD, "to know [ABLV's] comments on the OCCRP report, how this would happen given the fact 'strict capital controls,' what actions have been taken in the short and long run and when they will be implemented." Also in January 2017, an RM wrote in an email: "ABLV is at the moment part of

our network, however we will evaluate if they should remain going forward. Unfortunately, Nordea is exposed to AML risks related to ABLV Bank."

91. In March 2017, a Nordea Evaluation Board ("EVB") performed EDD on ABLV. Despite the reporting from OCCRP, the EVB elected for Nordea to continue its relationship with ABLV as a risk class "C" bank. The EVB recommended that Nordea conduct KYC on ABLV again before the end of 2017.

92. In September 2017, a Nordea employee from the BRIS Unit, reached out to both the Senior Relationship Manger ("SRM") for ABLV and to the head of the IB unit to inform them that ABLV "has been identified with transaction activities in the so-called Russian Laundromat investigations." The head of IB responded that "we have our eyes on the bank (and personally I do not like it)." They added that the SRM for ABLV would be visiting the bank in October of 2017 to conduct a site visit. Finally, in an email dated December 12, 2017, the SRM indicated that after visiting ABLV in October, they had decided "to close" the relationship with ABLV. However, a Nordea evaluation board EVB meeting in January 2018 indicated a desire to continue the ABLV relationship, with a rating of "very high risk."

93. At long last and on the same date that FinCEN issued its notice of proposed rulemaking pursuant to Section 311 of the PATRIOT Act, Nordea contacted ABLV to inform it that it would terminate this relationship. Nordea closed ABLV's Nordic currency correspondent accounts and RMA keys by February 27, 2018, having delayed in adequately responding to repeated red flags regarding the heightened risk of doing business with ABLV during the preceding four years.

Nordea's Correspondent Banking Relationships with Bank of Cyprus

94. Founded in 1899, and headquartered in Strovolos, Cyprus, Bank of Cyprus has had close associations with Russia and Vladimir Putin. Cyprus is known as one of Russia's favorite money havens.

95. Nordea provided a correspondent banking account to Bank of Cyprus in DKK between 2008 and December of 2019 and exchanged thirteen RMA keys with Bank of Cyprus in assorted currencies. The DKK account remained open until December 2019 due to an outstanding guarantee. Between 2008 and 2013, Nordea processed 17,427 U.S. dollar payments totaling approximately $91.76 billion through its relationships with Bank of Cyprus. Between 2008 and 2019, Nordea's New York Branch processed 613 U.S. dollar payments worth $19,680,215.30 involving Bank of Cyprus. Nordea's KYC files on Bank of Cyprus describe Nordea's "substantial payments flow" with Bank of Cyprus.

Nordea Performed Insufficient Due Diligence on Bank of Cyprus and Did Not Appropriately Address Red Flags

96. Nordea's KYC files on Bank of Cyprus dating back to 2013 identified high risks with the bank, designating it an AML risk class "C." In February 2013, Nordea judged the quality of Bank of Cyprus's AML/CTF and Sanctions management policies and procedures to be "weak" on the grounds that "[t]he bank's AML policy is not very specific." Nordea identified country-specific concerns regarding Cyprus, too, including that "Cyprus is on the edge of bankruptcy and is under suspicion for being a tax heaven [sic] for especially Russians."

97. Emails dating back to February 2013 reveal a general sense of caution within Nordea regarding banking in Cyprus. An SRM wrote in an email that "we are not allowed to take any risks in banks in Cyprus. I understand that they want to make deposits with Nordea. But we need to be 110% sure there is no risk involved when paying the money back to Bank of Cyprus."

Another RM wrote, "[t]he thing is that it has been decided that Cyprus is banned." By April 2013, Nordea had closed its RMA keys with all Cypriot banks save for three, one of which was Bank of Cyprus.

98. In 2015, Nordea's GIA performed sample testing of the 2013 and 2014 Bank of Cyprus KYC files and identified gaps in Nordea's KYC diligence on Bank of Cyprus. These gaps included that Nordea lacked current documentation on Bank of Cyprus; failed to archive supporting documentation for its rating of Bank of Cyprus; did not obtain biographies for Bank of Cyprus's newly appointed board; performed inadequate screening regarding PEPs; had not visited Bank of Cyprus in five years; and rerated Cyprus from a higher risk "C" country to a lower risk "B" country despite its risk rating in the relevant AML atlas remaining unchanged.

99. Nordea's 2015 KYC file on Bank of Cyprus identified additional red flags. With regard to country-specific AML risks, the file observed that Cyprus was classified "as an offshore financial center as well as a suspected money laundering country." Compounding this risk was the ineffectiveness of the Cypriot financial supervisory authorities, which the KYC file described as "understaffed and lack[ing] training." The KYC file also identified weaknesses in Bank of Cyprus's corporate structure and its policies and procedures. Nordea found that the "bank holds a large number of subsidiaries, involved in properties" which was "[n]ot a logical structure for a bank." Nordea again observed that "the bank's AML policy is not very specific" and would therefore be "classified as weak."

100. In addition, the 2015 KYC file noted that there were three PEPs on the board of Bank of Cyprus: one of those, Vladimir Strzhalkovsky, was a former KGB agent and a long-time close associate of Vladimir Putin. Another PEP on the board had faced extensive prior legal sanction in connection with his role at another bank.

101. The 2015 KYC file shows that Nordea did not conduct site visits for Bank of Cyprus, stating that "[t]he Bank has not been visited for the past 5 years, and we have not obtained information from the FSA or a-class bank, but this is not view [sic] a problem in terms of KYC approving the bank as all other documents are in order."

102. The conclusion section of the 2015 KYC file focused on the AML risks facing Bank of Cyprus, noting that "[a]llegations of money laundering of Russian money keep tuning [sic] up" and that "Cyprus has always been considered a tax heaven [sic] for Russians." Nordea retained its AML risk class "C" rating for Bank of Cyprus, with the KYC reviewer noting that the bank would continue to be monitored closely.

103. Nordea has been unable to locate its 2016 KYC file for Bank of Cyprus.

104. Nordea's 2017 KYC file on Bank of Cyprus identified money-laundering risks that the correspondent banking relationship presented and maintained the AML risk class "C" rating as in prior years. The file noted that Cyprus was "considered a tax haven"; that the level of regulatory supervision was weak; and that the bank had 217 wholly-owned subsidiaries, some of which were located in known tax havens and countries with high money-laundering risks such as the Channel Islands, Guernsey, and Cyprus. Bank of Cyprus's engagement in high-risk "occasional transactions" businesses such as cash currency transactions and its services to walk-in customers were also flagged as risks. The KYC file further reflects that Nordea "never met the bank" due to its low business volume and business potential.

105. Nordea's 2018 KYC file for Bank of Cyprus contained information about Bank of Cyprus's customer base and services including that it was still offering risky "occasional" services such cash currency transactions for walk-in customers, including tourists; and that it was providing services to online gambling companies.

106. In February 2019, Nordea's International Banks and Countries Credit Committee decided that Nordea's relationship with Bank of Cyprus should be closed. Justifications for this decision included "the financial crime risks and concerns relating to Cyprus as an offshore jurisdiction with links to high-risk activities such as online gambling, shipping, and financial holding companies," as well as "low business volumes" in the region. Ultimately, Nordea closed down all of its RMAs with Bank of Cyprus except for those it was required to maintain because of prior guarantees it had entered into with Bank of Cyprus. The last of those guarantees expired in 2023, at which point Nordea was able to fully exit the relationship.

107. Notwithstanding Nordea's longstanding concerns about Bank of Cyprus, including the geographic risks, the bank's poor governance, inadequate internal controls, and high-risk business practices, Nordea waited until 2019 to make the decision to end this relationship.

Transaction Monitoring

108. Nordea first acquired an IT-supported transaction monitoring system in 2008, which it technically fully introduced in 2010. Nordea's main automated transaction monitoring tool was called the FACP. FACP initially contained three transaction monitoring scenarios, increasing to six scenarios by 2013, although none of these targeted scenarios dealt with correspondent banking transactions, a problem highlighted by an S-FSA May 2015 order.

109. In that order, the S-FSA found, *inter alia*, that "it has been established that Nordea has not had a sufficiently efficient system and procedures to monitor transactions for several years" and that Nordea's "sub-standard monitoring of transactions and its unsatisfactory customer due diligence information has meant that in all likelihood suspicious transactions could have passed through the Bank's operation unnoticed."

110. In 2016, Nordea began rectifying the problems highlighted by the S-FSA by implementing transaction monitoring scenarios designed to specifically target risks posed by correspondent banking relationships, ultimately implementing 28 such scenarios. However, implementation of the automated FACP system proved problematic at Nordea Bank Finland. As Nordea explained to Finnish regulators in July 2017, transaction data for Nordea Bank Finland's Loro and Nostro accounts were not sourced to Nordea's automated transaction monitoring system. Accordingly, Nordea's automated transaction monitoring system was not initially able to include Nordea Bank Finland. To mitigate the limitation identified in Finland, Nordea began to develop semi-automated controls (also known as "manual typologies"), which were implemented by Q2 2018.

111. Nordea's Group Compliance Report for the first quarter of 2018 identified several areas of concern pertaining to transaction monitoring that contributed to Nordea's overall AML risk being scored critical.

112. In addition to automated transaction monitoring systems, Nordea employed manual transaction monitoring processes in three different tools: the SWIFT Analyzer; the SWIFT Compliance Analytics Report; and the SMARTI report.

Nordea Failed to Stop Transactions in its Correspondent Banking Relationship with ABLV After FinCEN's Notice of Proposed Rulemaking

113. Nordea failed to stop three payments involving ABLV after FinCEN issued a notice of proposed rulemaking, designating ABLV as an institution of primary money laundering concern, owing to lags in Nordea's updates of its internal lists of FinCEN 311 entities. The failure to stop these payments led to breaches of Nordea's internal sanctions standards, and in one instance, led a Nordea employee to raise concerns about a potential breach of the PATRIOT

Act. Nordea responded to these issues once they were identified and used the lessons learned to improve its transaction monitoring processes.

114. For example, a Nordea incident report filed on February 20, 2018, described a case in which ABLV instructed a transaction for a customer on February 16, 2018, in which Nordea Norway acted as the NOK correspondent bank. The transaction was ultimately returned to Nordea for cancelling by a different bank, on the grounds that ABLV had previously been designated a FinCEN 311 bank.

115. Nordea employees attributed the failure to stop the transaction to logistical delays in updating its list of FinCEN 311 entities. Specifically, Nordea used manually updated, internal lists of FinCEN 311 entities and did not source a FinCEN 311 list from an external provider. Accordingly, even though FinCEN's notice of proposed rulemaking designated ABLV as a 311 entity on February 13, 2018, this designation did not appear on Nordea's internal list on February 16, 2018, allowing the transaction to occur contrary to internal policy.

116. Delays in Nordea's updates of its internal FinCEN 311 list led to a similar incident in which Nordea failed to stop transactions involving ABLV this time in two U.S. dollar transactions. Nordea classified this incident internally as "Major/Severe" and a "breach of FINCEN/311 Patriot Act." Specifically, on February 20, 2018, a U.S. bank returned two U.S. dollar payments – one made on February 13, 2018, and the other February 16, 2018 – to Nordea that involved ABLV. When the U.S. bank returned the two payments, Nordea did not initially treat this event as an "incident," owing to internal "confusion" about what exactly happened. But when Nordea subsequently detected there was an incident, it took active steps to stop these problematic payments in March 2018.

117. Here, once again, the cause for this incident was Nordea's reliance on manually-updated internal lists of FinCEN 311 entities that were not updated in a timely manner, thus allowing the transactions to occur when they should not have.

Nordea Failed to Adequately Respond to Transaction Monitoring Alerts Involving Bank of Cyprus

118. Between 2016 and 2018, Nordea's transaction monitoring systems alerted Nordea to transactions involving Bank of Cyprus. Nordea employees debated whether to file an Unusual Activity Input in connection with these flagged transactions but ultimately decided not to. On one occasion, Nordea employees considered whether the relationship with Bank of Cyprus should be terminated on account of these suspicious transactions, ultimately deciding against doing so.

119. For example, in May 2017, Nordea employees identified suspicious payment activity in connection with Bank of Cyprus's DKK account with Nordea. While Nordea's SRM for Bank of Cyprus aptly requested additional clarifying information from Bank of Cyprus, there is no indication that Nordea ever received a response from Bank of Cyprus. Moreover, on May 3, 2017, Nordea personnel discussed internally whether to file an Unusual Activity Input in connection with these suspicious transactions and even whether Nordea should terminate its relationship with Bank of Cyprus in light of them. Ultimately, however, no Unusual Activity Input was filed in connection with these transactions, and Nordea did not terminate its relationship with Bank of Cyprus until 2019.

Nordea's 2018 Group Compliance Report's Findings Regarding Transaction Monitoring

120. Nordea's 2018 Q1 Group Compliance Report rated Nordea's overall AML risk as "critical," partly due to concerns with Nordea's transaction monitoring. The report found that

"improvements [were] required in transaction monitoring scenarios" and there were "backlogs in TM investigations." The report identified transaction monitoring backlogs both in Nordea's first and second lines of defense. These concerns contributed to an overall AML risk of "critical."

Issues Related to Nordea's Transaction Monitoring of Luminor Transactions

121. As described previously, Nordea maintained an active AML role with respect to Luminor, including regarding transaction monitoring. Also, in 2017-2018, Nordea received inquiries from banks in its correspondent banking network, including its dollar-clearing bank in the Baltics, regarding Luminor transactions. While investigating these inquiries, Nordea employees identified shortcomings in Nordea's own transaction monitoring systems.

122. For example, in December 2017, a U.S. dollar clearing bank sent six U.S. dollar transaction monitoring inquiries to Nordea regarding Luminor transactions. Analyzing the transactions, a Nordea employee concluded that "Nordea cannot be comfortable with Luminor in terms of risk appetite, understanding of red flags including lack of knowledge of ML [money laundering] typologies and further, breach of bank secrecy rules." Replying, Nordea's Global Head of IB wrote in an email that they would "buy some time at [U.S. dollar clearing bank] so we find out how to deal with this." They added that "[U.S. dollar clearing bank] might be concerned why Nordea didn't find there [sic] transactions suspicious ourselves, ie they didn't come out in Nordea's own automated Transaction Monitoring Alerts which clearly shows our Transaction Monitoring is not up to [U.S. dollar clearing bank]'s standards." A March 2018 progress report on Project Lux regarding USD transactions in Nordea/Luminor showed that the overall volume of USD transactions at Luminor started to decrease, and that Luminor had introduced a restriction on opening USD accounts for newly onboarded customers, with exceptions only granted with pre-approval from Luminor's Head of AML. At an October 2018

Project Lux Steering Group meeting, Nordea identified transaction monitoring enhancements to mitigate its AML risk exposure in Luminor domestic and international transactions.

Cooperation and Remediation

123. The Department has given substantial weight to Nordea's extensive cooperation with the Department throughout this investigation. This cooperation has included Nordea's timely and appropriate responses to requests for information and its support to provide relevant information through a novel channel created by the FIN-FSA. Additionally, the Department recognizes Nordea's efforts to remediate the historical deficiencies identified in this Consent Order, which included a substantial and continued financial investment into compliance resources and risk-based enhancements to its compliance program.

Violations of Law and Regulations

124. Nordea failed to maintain an effective and compliant anti-money laundering program, in violation of 3 N.Y.C.R.R. § 116.2.

125. Nordea failed to conduct adequate due diligence in its correspondent bank and RMA relationships in violation of 3 N.Y.C.R.R. § 116.2.

126. Nordea failed to maintain an adequate transaction monitoring system in violation of 3 N.Y.C.R.R. § 504.3.

NOW THEREFORE, to resolve this matter without further proceedings, the Department and the Bank stipulate and agree to the following terms and conditions:

SETTLEMENT PROVISIONS

Monetary Provisions

127. Nordea shall pay a civil monetary penalty pursuant to Banking Law §§ 39 and 44 to the Department in the amount of thirty-five million U.S. dollars ($35,000,000.00) within ten

(10) days of executing this Consent Order. The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department. Nordea agrees that its members will not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

Full and Complete Cooperation of Nordea

128. Consistent with applicable law, Nordea commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order.

Breach of Consent Order

129. In the event that the Department believes any party to this Consent Order to be in material breach of the Consent Order, the Department will provide written notice to the party, and the party must, within ten (10) business days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

130. The parties understand and agree that the party's failure to make the required showing within the designated time period shall be presumptive evidence of the party's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all the remedies available to it under New York Banking and Financial Services Law and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Waiver of Rights

131. The parties understand and agree that no provision of this Consent Order is subject to review in any court or tribunal outside the Department.

Parties Bound by the Consent Order

132. This Consent Order is binding on the Department and Nordea Bank Abp and its New York Branch as well as any successors and assigns that are under the Department's supervisory authority. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

133. No further action will be taken by the Department against Nordea Bank Abp and its New York Branch for the conduct set forth in the Consent Order, provided that Nordea Bank Abp and its New York Branch comply with the terms of the Consent Order.

134. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against Nordea Bank Abp and its New York Branch for transactions or conduct that was not disclosed in the written materials submitted to the Department in connection with this matter.

Notices

135. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Avery Heisler
Assistant Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

Christina Glekas
Assistant Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

Joseph C. Mineo
Excelsior Fellow for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One Commerce Plaza
Albany, NY 12210

Ching-Huei Li
Excelsior Fellow for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For Nordea Bank Abp and Nordea Bank Abp New York Branch

Jussi Koskinen
Chief Legal Officer
Nordea Bank Abp
Head Office

Jamie Graham
Chief Compliance Officer
Nordea Bank Abp
Head Office

Henrik M. Steffensen
Executive Vice President and General Manager
Nordea Bank Abp
New York Branch

Ryan D. Junck
Skadden, Arps, Slate, Meagher & Flom LLP
Counsel to Nordea

Miscellaneous

136. This Consent Order and any dispute thereunder shall be governed by the laws of the State of New York without regard to any conflicts of laws principles.

137. This Consent Order may not be altered, modified, or changed unless in writing and signed by the parties hereto.

138. This Consent Order constitutes the entire agreement between the Department and the Bank and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order.

139. Each provision of this Consent Order shall remain effective and enforceable against the Bank, its successors, and assigns, until stayed, modified, suspended, or terminated by the Department.

140. In the event that one or more provisions contained in this Consent Order shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

141. No promise, assurance, representation, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of the Consent Order.

142. Nothing in this Consent Order shall be construed to prevent any consumer or any other third party from pursuing any right or remedy at law.

143. This Consent Order may be executed in one or more counterparts and shall become effective when such counterparts have been signed by each of the parties hereto (the "Effective Date").

[*rest of page intentionally left blank***]**

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s/ Elizabeth A. Farid
ELIZABETH A. FARID
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement

August 27, 2024

By: /s/ Kathryn A. Taylor
KATHRYN A. TAYLOR
Deputy Director of Enforcement
Consumer Protection and Financial Enforcement

August 27, 2024

By: /s/ Christopher B. Mulvihill
CHRISTOPHER B. MULVIHILL
Deputy Superintendent for Consumer Protection and Financial Enforcement

August 27, 2024

By: /s/ Samantha R. Darche
SAMANTHA R. DARCHE
Acting Executive Deputy Superintendent
Consumer Protection and Financial Enforcement

August 27, 2024

NORDEA BANK ABP

By: /s/ Jussi Koskinen
JUSSI KOSKINEN
Chief Legal Officer

August 21, 2024

By: /s/ Jamie Graham
JAMIE GRAHAM
Chief Compliance Officer

August 21, 2024

NORDEA BANK ABP NEW YORK BRANCH

By: /s/ Henrik M. Steffensen
HENRIK M. STEFFENSEN
Executive Vice President and General Manager

August 22, 2024

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

By: /s/ Ryan D. Junck
RYAN D. JUNCK
Counsel to Nordea

August 21, 2024

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services

August 27, 2024